

# Implementing ITIL with Kaseya Tools

A white paper by Robert Perrine, ITIL-Service Manager



## Executive Overview

Kaseya Service Desk provides the logic and tools necessary to guide a company into ITIL – the most widely used standard for the efficient operation of an IT organization. Kaseya Service Desk tools are intuitive and easy to use. The goal for this suite is to give you ITIL in a box. This release includes Incident Management, Service Request Management, Problem Management and Change Management.

## Introduction

ITIL<sup>1</sup> stands for Information Technology Infrastructure Library. The ITIL standard describes best practices for IT. ITIL began as a British standard. Now the core elements of ITIL are a world-wide standard through ISO 2000 from the International Standards Organization.

ITIL defines the roles and responsibilities for an IT organization. For example, ITIL separates the duties of rapidly responding to incidents from the responsibility for proactive problem prevention. The reason for doing this is to help people focus. The rapid responders need to be always at the ready. They cannot get tangled up in complex problems that will take weeks to research. And the people doing the difficult research need to be protected from interruptions. ITIL defines Incident Management and Problem Management as distinct disciplines and gives each clear direction on what to do.

The roles within ITIL describe how to organize an IT shop for efficiency. The problem is that most IT organizations today are not aligned with ITIL. And transitioning into a new organizational structure is difficult work. What companies need is a tool to help them through the transition into ITIL. The minimum requirement for such a tool is the ability to clearly separate the duties of Incident Management, Service Request Fulfillment, Problem Management and Change Management.

**Kaseya Service Desk is one tool that gives an IT organization ITIL in a package.**

<sup>1</sup> ITIL compliance is a process and method of doing business that each IT team must implement, manage and monitor for itself. And while Kaseya Service Desk customers have a huge leg up with a cutting edge ITIL compliance tool, the mere use of Kaseya products or services does not give or guarantee ITIL compliance. It is the sole responsibility of each customer to understand the ITIL compliance rules and process and to implement, manage and monitor any ITIL compliance efforts for the Customer's own account. Kaseya does not offer ITIL compliance services or advice and the content contained in this whitepaper is provided for informational purposes only and without warranty of any kind. Kaseya will have no liability relating to any ITIL compliance efforts or the content of this whitepaper.

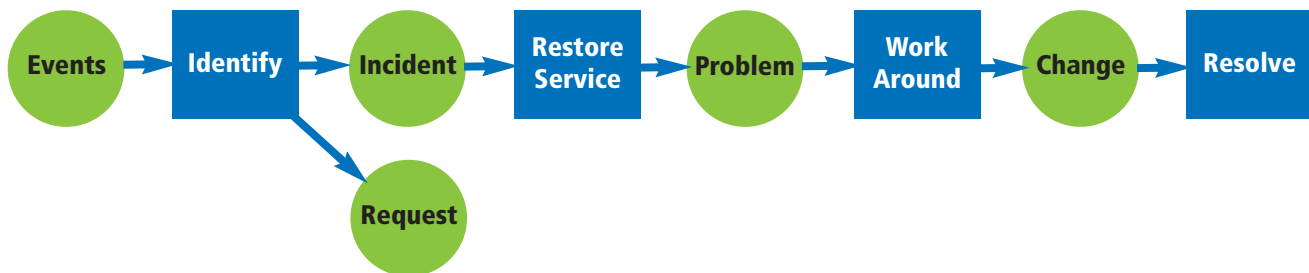
## Service Desk

An ITIL Service Desk is the single point of contact for the people that use IT services. Monitoring events, telephone calls, email, requests for status and requests for service all route through the Service Desk.

The first priority for the people working the Service Desk is to identify the nature of the message. Is the person calling to report a new incident, or check on the status of an open incident? Has the incident been worked and turned into a problem? And where is the change that is going to resolve the problem? The Service Desk needs one tool with all the answers. And yet, for efficiency, the specialists working the incidents, problems and changes need compartmentalization so they can focus. The Kaseya Service Desk meets both needs. The Kaseya Service Desk consolidates incidents, requests, problems and change into one tool. And the Kaseya Service Desk provides specialization for each type of ticket.



To understand the ITIL view of consolidation and specialization it is important to understand the ITIL life cycle for an event. As shown, below, an event can be identified as an Incident. The goal for Incident Management is to restore service with minimal disruption. The underlying problem then goes to Problem Management who is responsible for devising a work around and then creating a change that will permanently resolve the problem.



For example, an automated monitoring event is sent to Service Desk reporting that a web service is exceeding the threshold set for a page to display. The Incident Management team sees the event, checks the server and notices that one of the services is hung. The Incident response team restarts the service and the web server begins displaying pages again. If this happens once every couple months no one is likely to be concerned. If, however, this starts happening once a day or multiple times a day then the Incident Management team should open a problem ticket. The Problem Management team will triage the situation and find a work around. For example, they might set the service to automatically restart every night at 1am. If the problem is severe enough they will need to dig deeper, find the root cause and fix it. That fix might be a service patch or a significant redesign. Before that fix can go into production the Problem Management team will open a Request for Change (RFC) and work with the Change Management team to get authorization. After the change is implemented the cycle starts over.

All of this information needs to be in one tool. From the customer's perspective the web server either works or it does not. The customer is not concerned about how IT does their job. So when the customer calls they do not want to get bounced around from department to department while everyone says someone else is working on it. The customer wants to call one place and get the latest status. The place they should call is the Service Desk. And the Service Desk technician who answers that call should expect to find all the relevant information in one tool – the Kaseya Service Desk.

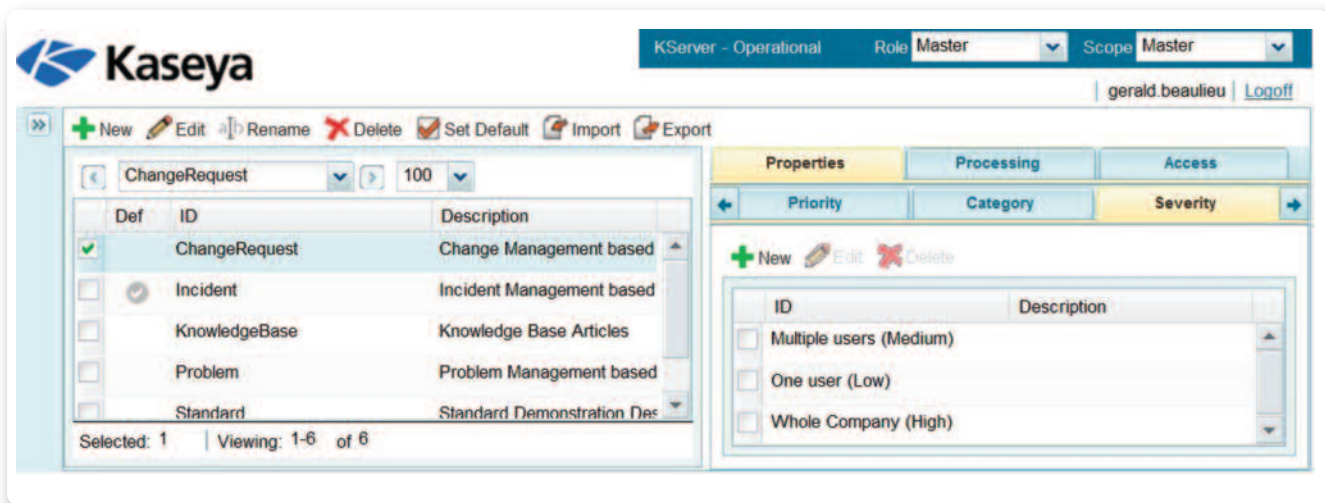
## Incident Management

Incident Management is the ITIL discipline that deals with disruptions. Monitoring software is generally deployed to detect and report events. Your customers also use the telephone, email, IM and whatever else they have at hand to tell you when something is not working right. The goal of the Kaseya Service Desk for Incident Management is to bring all of that information together in one place where it can be prioritized. When something bad happens you want to know that the right people are working on the right tasks. Service Desk for Incident Management lets you know what is happening.

The goal for a Service Desk is to be more than just a call center. First, an incident needs to be captured. Monitoring events, phone calls, emails and everything else need to be brought together into one system.

Then all of this information needs to be filtered and categorized. Events sent in from monitoring tools and trouble reports from customers are all Incidents. Requests for standardized work are Service Requests. Incidents need immediate attention while Service Requests can be scheduled. For example, if a customer calls to say that his or her laptop cannot connect to the network, someone needs to review and triage the issue. If the problem is that the network is down, then this is an Incident that will probably route over to the network support group. If the problem is that the customer forgot his or her password, then this is a Service Request that can probably be handled by the Service Desk. And if the issue is that the customer is again requesting wireless connectivity in a wired facility then this phone call might be best classified as a Request for Change. This initial categorization ensures that the work gets to the right person. Kaseya Service Desk makes this categorization easy.

The next step is to prioritize the work. ITIL defines prioritization as the sequence in which tasks should be worked based on the impact to the organization and the urgency of the need. Kaseya Service Desk recognizes severity, urgency and priority.



**Add Custom Field** ? □ ×

**■** Define custom fields and add them to the service desk definitions. When a ticket is created based on a service desk definition, custom fields assigned to the service desk are available for data entry in the ticket. Reports can display and be organized by the custom fields you create. Service desk procedures can reference the values contained in custom fields to perform a task.

ID\*:

Screen Caption\*:

Report Title:

Field Format\*:

Default Value:

Value to Add to List:

Values Added to List:

**Values Added to List**

High

Low

Medium

KServer - Operational
Role **Master**
Scope **Master**

gerald.beaulieu | [Logoff](#)

»»

ChangeRequest
100

Def	ID	Description
<input type="checkbox"/>	ChangeRequest	Change Management based on ITIL
<input checked="" type="checkbox"/>	Incident	Incident Management based on ITIL
<input type="checkbox"/>	KnowledgeBase	Knowledge Base Articles
<input type="checkbox"/>	Problem	Problem Management based on ITIL
<input type="checkbox"/>	Standard	Standard Demonstration Desk
<input type="checkbox"/>	Standard_Desk_Desko	Standard SD

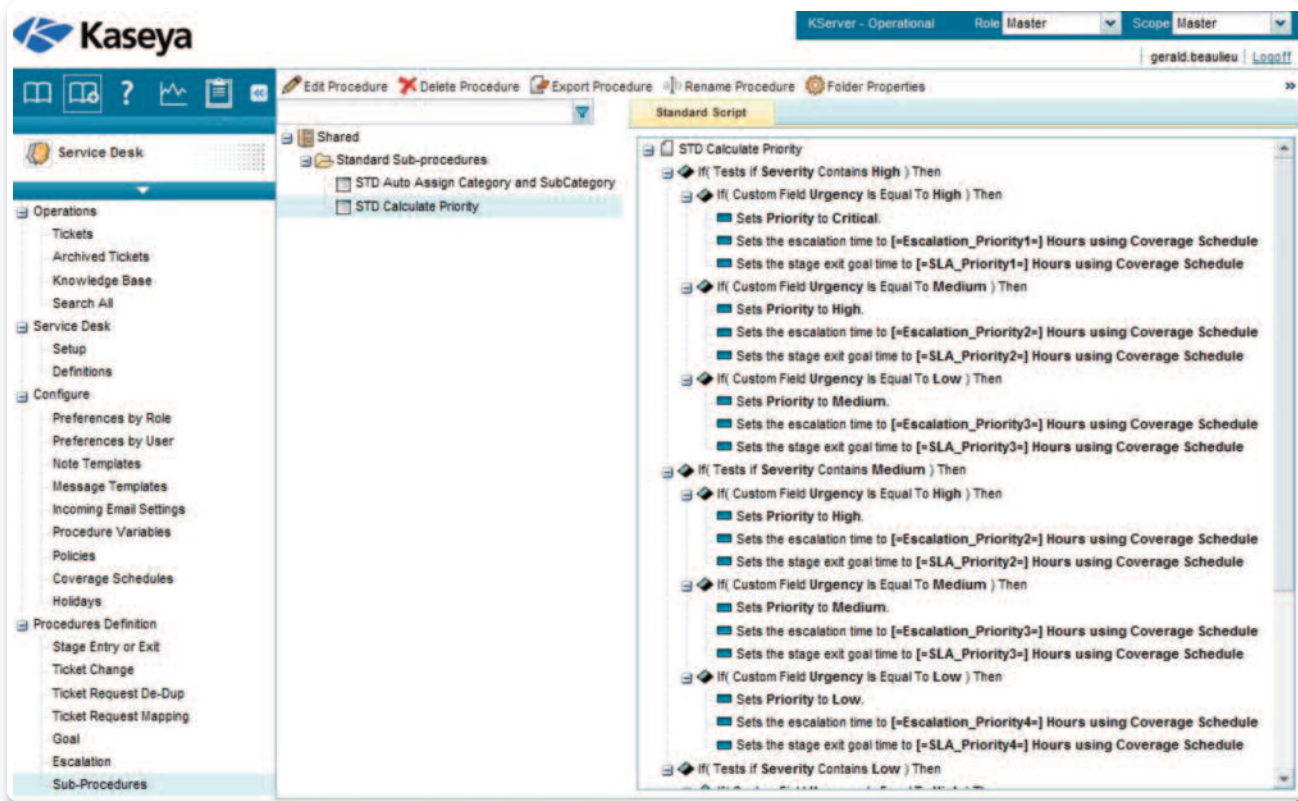
Selected: 1 | Viewing: 1-6 of 6

+ Properties
Processing
Access

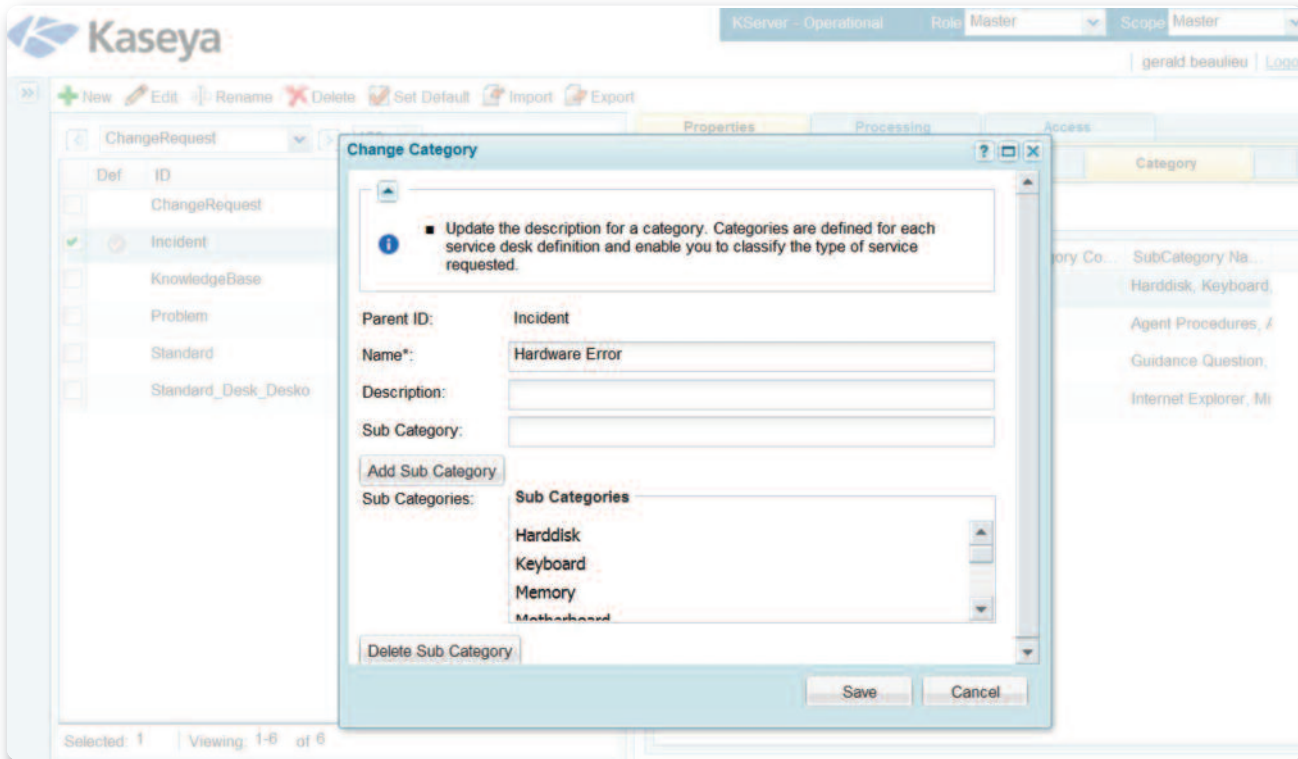
← Status
Priority
Category

+ New
Edit
Delete

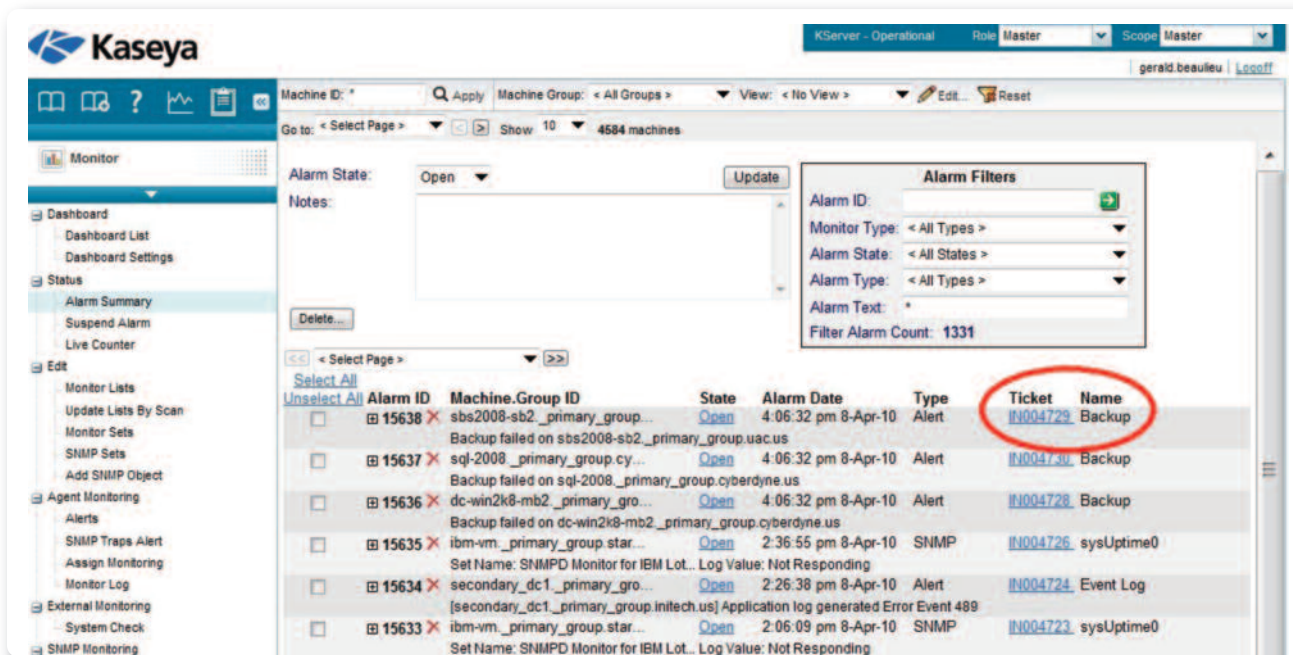
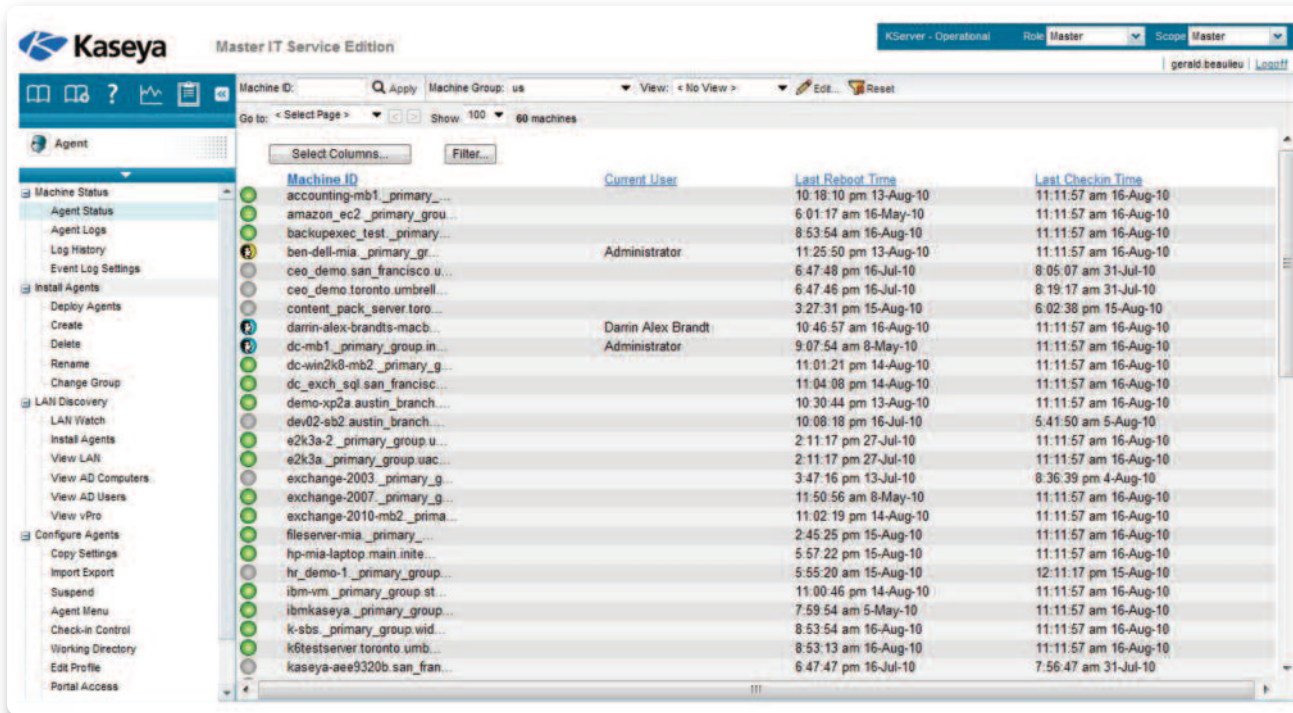
ID	Description
<input type="checkbox"/> Critical	1 hour target resolution time
<input type="checkbox"/> High	8 hour target resolution time
<input type="checkbox"/> Low	48 hour target resolution tim
<input type="checkbox"/> Medium	24 hour target resolution tim
<input type="checkbox"/> Planning	Planned



Capturing the information and categorizing the issue is the first step in Incident Management.

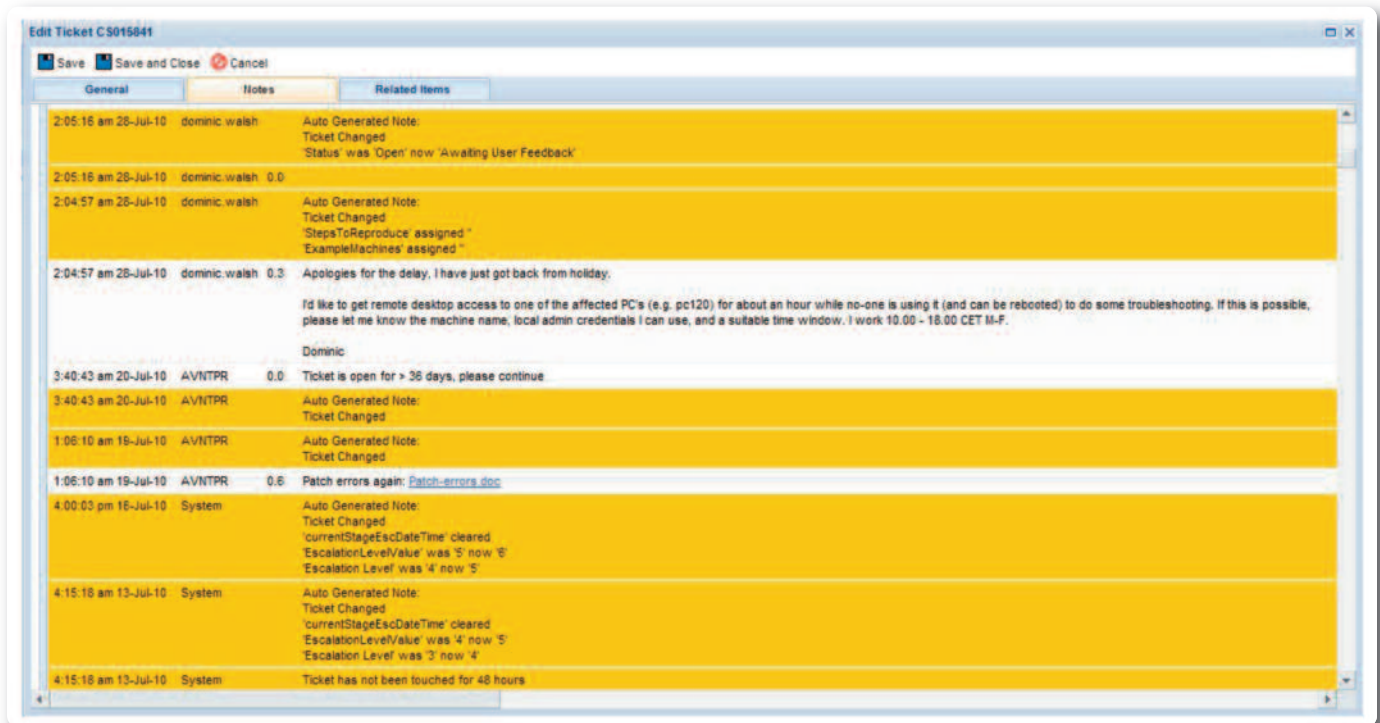


The next step is to do an initial diagnosis. The goal here is to successfully resolve as many Incidents as possible within the Service Desk. Kaseya Service Desk is an ideal tool for this purpose because it leverages the power of the Kaseya monitoring and management suite.

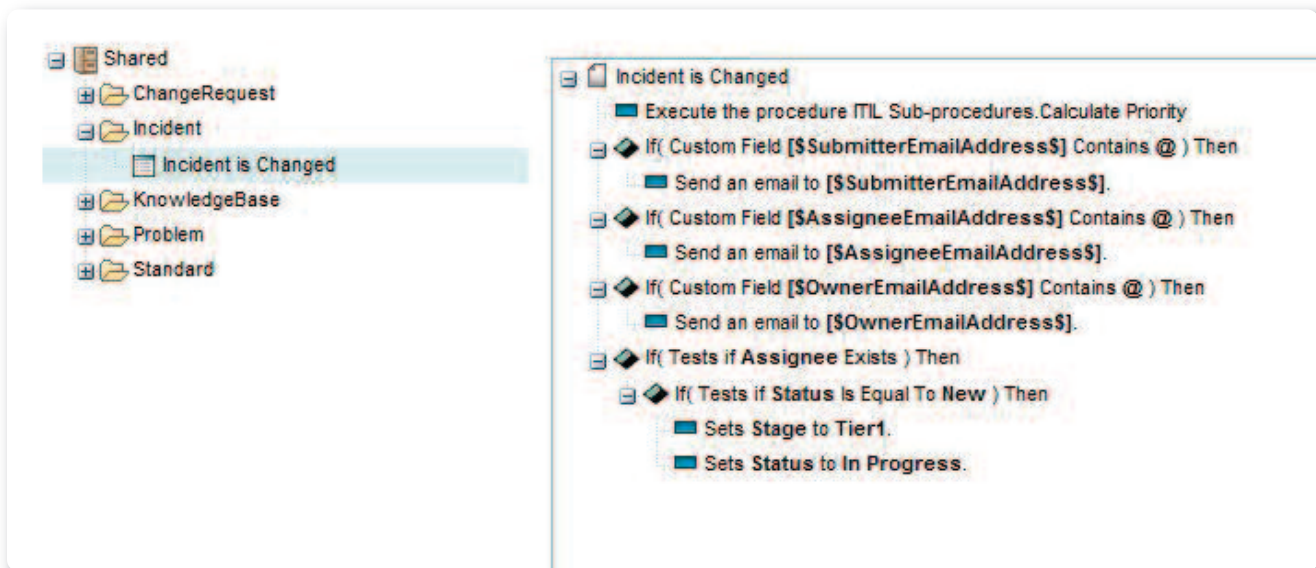


From within the Incident Service Desk an analyst can immediately see the history and performance of the system responsible for the Incident. The analyst can immediately run scripts to troubleshoot and resolve problems. Or the analyst can connect through the Kaseya tools and get onto the system to make corrections. The ITIL goal for Incident Management is to resolve Incidents as quickly as possible. The business goal for IT is to work as efficiently as possible. Kaseya Service Desk hits the mark on both objectives.

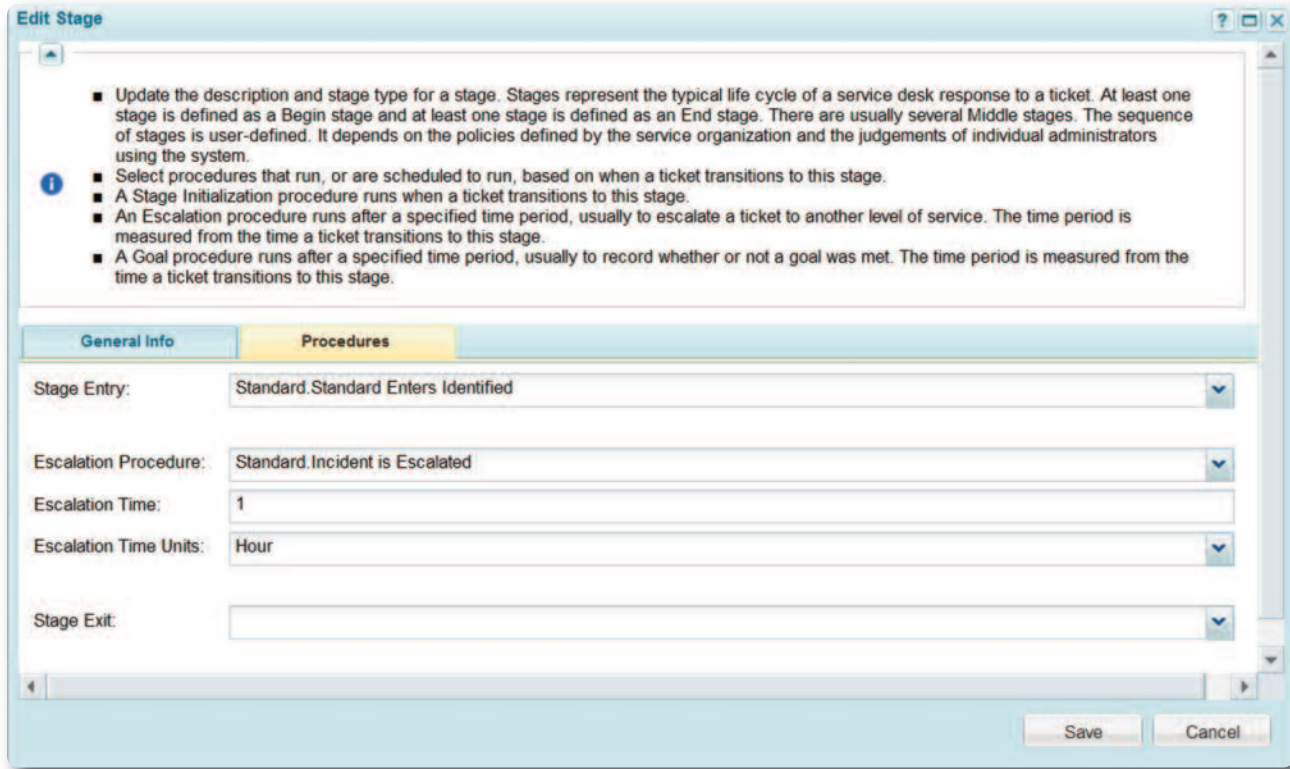
Kaseya Service Desk is also the platform for collaborative efforts. Each analyst can see the steps taken by others working on this Incident through the work notes.



The Kaseya Service Desk also includes extensive automation options so that notifications and/or corrective actions can be predefined to trigger automatically.



If the Incident needs to be escalated upward to management, then the work notes tell the history of what has been done. And if the Incident needs to be escalated laterally to another technical group, then the work notes give the technical people a way to share information.



Incidents are detected, documented, categorized, prioritized and worked to resolution. The ITIL process for Incident Management is shown below. And when everything works correctly IT becomes a service that is taken for granted.



Reporting then helps IT demonstrate the value of the IT services. The Kaseya reports on Incidents document the volume of work that is efficiently managed by IT. The reports can be formatted as text, uploaded into Excel or displayed as charts. The data within the reports progresses from a high level overview, down to details about each Incident. Examples of two high-level reports are shown below.

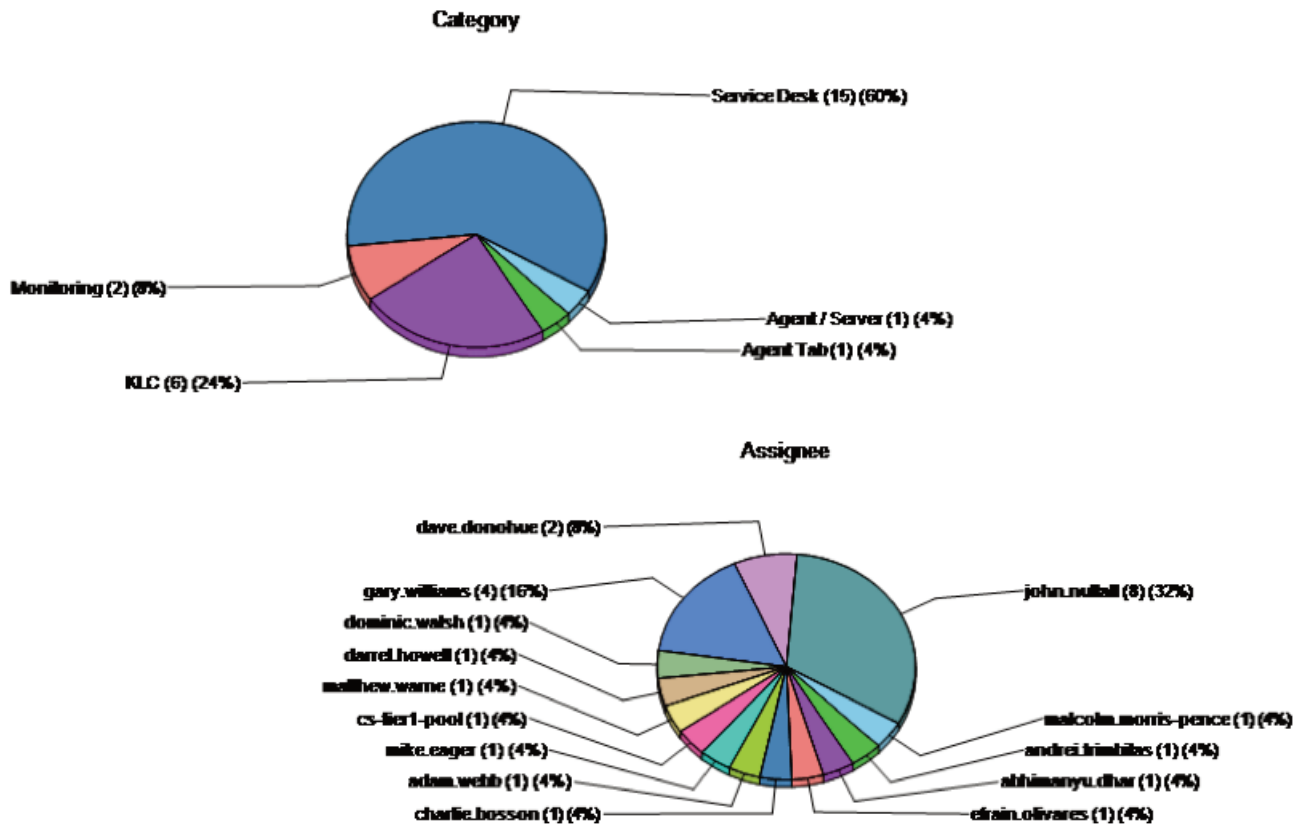
Ticket Status Summary	
Open Tickets	5
Ticket Closed Ticket	20
Past Due Tickets	0
Total Tickets	25

Tickets Issued				
0-30 days	30-60 days	60-90 days	> 90 days	Total
25	0	0	0	25
Tickets Closed				
0-30 days	30-60 days	60-90 days	> 90 days	Total
13	0	0	0	13
Ticket Resolution Time				
0-2 days	2-7 days	7-30 days	30-60 days	> 60 days
4	0	0	0	0
Past Due Tickets (Time Duration Unresolved)				
0-2 days	2-7 days	7-30 days	30-60 days	> 60 days
0	0	0	0	0

An example of the type of details available in an Incident report is shown in the following example.

Ticket #	Summary	Machine ID	Assignee	Priority	Modified Date	Creation Date	Submitter
CS011804	ticket escalation looking at holiday		gary williams				h.denboer@ncautomatisering.nl
	Service Desk		Open	All Endpoints Affected	5:44:09 PM 7-May-10	5:13:17 PM 4-May-10	
CS010851	check machine online/offline procedure		gary.williams				h.denboer@ncautomatisering.nl
	Service Desk		Ticket Closed	One Endpoint Affected	10:49:22 AM 30-Apr-10	7:22:25 PM 26-Apr-10	
CS010751	K2 server DOWN !!!		darrel.howell				h.denboer@ncautomatisering.nl
	Agent / Server		Ticket Closed	All Endpoints Affected	8:53:58 PM 28-Apr-10	7:08:01 AM 26-Apr-10	
CS009828	live connect from within ticket		mike.eager				h.denboer@ncautomatisering.nl
	Service Desk		Ticket Closed	One Endpoint Affected	7:16:18 AM 21-Apr-10	11:39:17 AM 19-Apr-10	

Summary and detail data can also be displayed graphically.

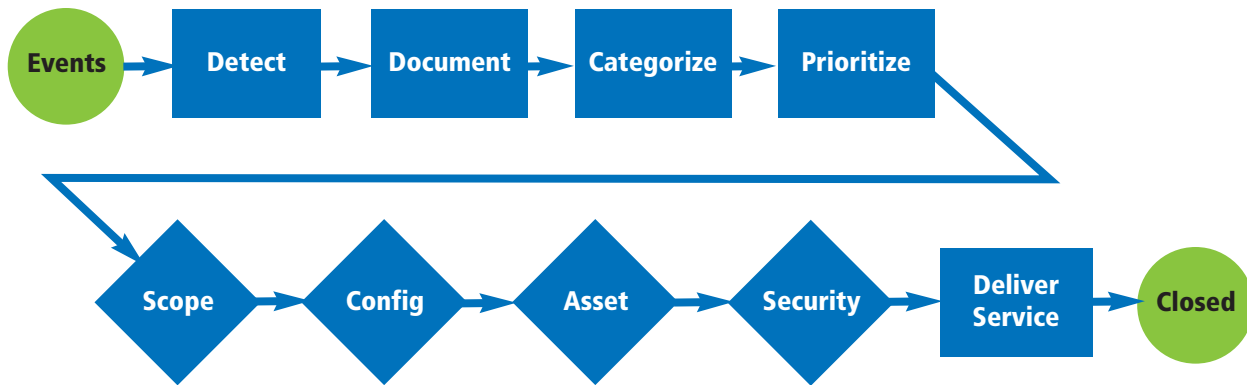


## Service Request Fulfillment

A service request is a request for a standard service. One of the most common service requests is a request to have a password reset. A service request is distinguished from an incident by determining whether or not normal services have been degraded. When a customer forgets his or her password the services delivered by IT are still in place. IT is still fulfilling its contract. However, the customer needs a change in the IT service before he or she can benefit from those services. Therefore the customer requests a change called a password reset.

A service request is not an incident and not a request for change. Requests for change need to go through the Change Management approval cycle. Service requests are managed by IT through an agreement that specific types of changes can be made without going through the change approval cycle. Installing software is an example of a type of change that might or might not need to go through the Change Management process. If a customer needs to have spreadsheet software added to their desktop they should open a service request. Adding the standard spreadsheet application to a desktop might raise concerns with Security Management or Asset Management but it is not likely to need to be reviewed by Change Management. Adding the standard spreadsheet application to a web server, however, should raise concerns with Security Management, Asset Management and Change Management. The difference is in the potential for risk. Minor changes to desktops are isolated and the system can be disconnected from the network if necessary. Configuration changes to shared resources always involve risk.

A customer might open a service request to add more memory to their laptop. An administrator, however, cannot use the service request route to bypass change management when they want to add more memory to the corporate financial database cluster.



The diagram shown above illustrates the service request process.

This process is a hybrid. The request may sound like an incident when the customer calls. Then, once we know it is a request, a flag is set that distinguishes Incidents from Service Requests. Thereafter the request follows a path similar to a change with layers of approvals.

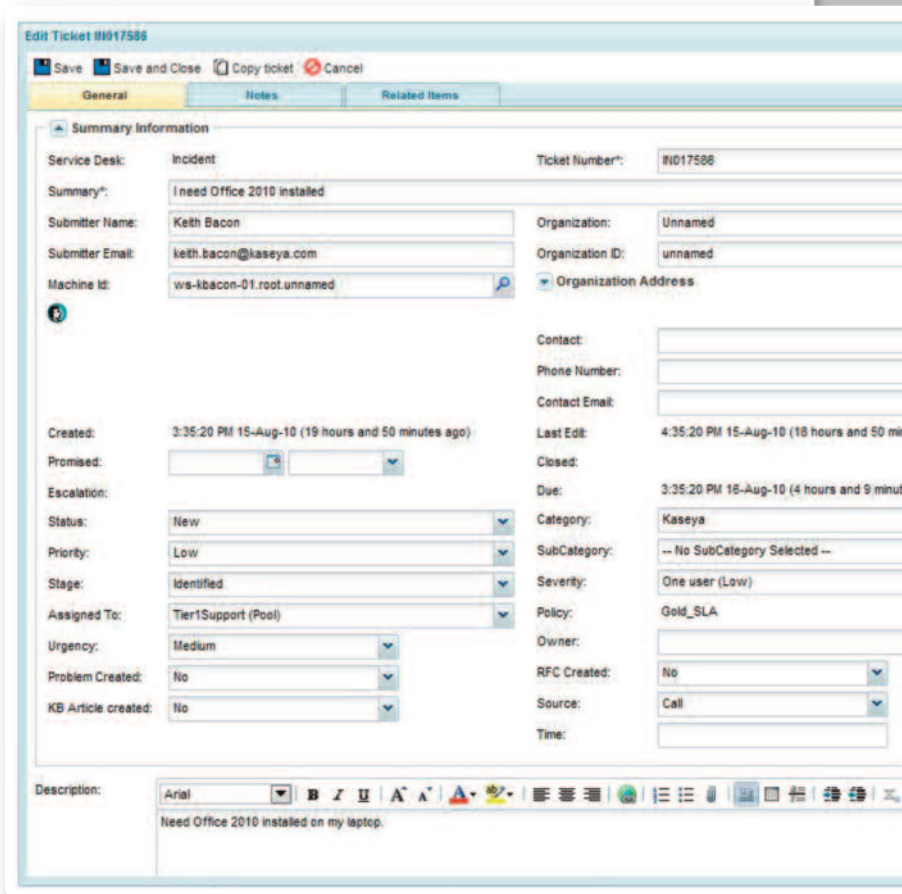
For example, a customer may request that the Service Desk kick off a standard set of month end reports. If the process is pre-defined then this request could be within the scope for what the Service Desk delivers. That same customer, however, may call and request that the Service Desk kick off a process to defragment a production database. And while starting a job to run a report and starting a job to defragment a database might have a lot of overlap, one might be within the scope for what the Service Desk does and the other might be something that is handled by specialists.

Exceptions to the configuration are specific to each environment. High security or highly regulated environments might forbid modifications to the desktop. Other environments might allow all of the users to manage their own laptops.

Asset Management needs to be involved when the request means that someone is going to use a corporate resource. Adding a little more software to a few desktops might not seem like a problem until the software vendor runs an audit to verify license compliance.

Security Management might forbid access to webmail accounts to reduce the risk of insider trading or intellectual piracy. Or Security Management might decree that webmail is the only tool authorized for business-to-business communication through an industry portal because this is the tool that is believed to minimize risk for that purpose. Service Requests need to be pre-defined so that the Service Desk knows what is allowed and which require special handling.

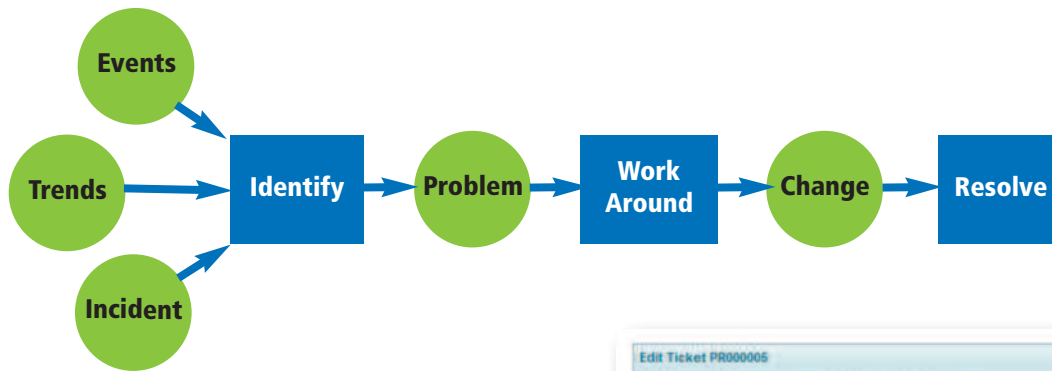
It is because service requests are not incidents and not requests for change that they need to be tracked and reported separately. The Kaseya Service Desk for Service Requests delivers the functionality required to implement Service Request Management.



## Problem Management

The goal for problem management is to permanently resolve the root cause of a symptom. Events detected by monitoring software, incidents reported by customers and trends detected by the IT staff are all symptoms. A reports server might generate events when reports fail. A customer might report an incident when their daily reports are truncated. And the system administrator might have difficulty logging on because of some underlying problem. The failed reports can always be re-run. The truncated reports can be run again. And perhaps the problem with logging on can be resolved by clearing out the temp directory. But all of those work-arounds take time and consume IT bandwidth.

The service performed by Problem Management is to find the common thread that connects symptoms, document a work-around and then find a permanent solution.



Problems need to be documented, tracked and worked. Incidents, events and even other problems should be linked to the problem that is being worked. The Kaseya Service Desk for Problem Management gives IT a tool to consolidate and disseminate all this information.

For example, the incidents on the reports server might all stem from the same problem with the temp directory getting full. Once someone can see the common theme then a work-around can be put in place to clear out the temp directory just before the nightly reports start running. That work-around might eliminate the symptoms and thus improve the quality of service. But it is just a work-around. Someone should find out why the temp directory keeps filling.

Within a typical IT organization there are lots of problems that need to be solved. And it is not uncommon for everyone to pick the problem they like best and delve into possible solutions. In a small shop that probably works. As the number of problems keeps increasing, however, it soon becomes necessary to prioritize the work. The Kaseya Service Desk for Problem Management makes that possible.

An example of the data entered to document an example problem is shown above.

Edit Ticket PR000005	
Save	Save and Close
Copy ticket	Cancel
General	Notes
Related Items	
Summary Information	
Service Desk:	Problem
Ticket Number:	PR000005
Summary*:	The Exchange servers are running on different domains
Submitter Name:	gerald
Organization:	Unites States
Submitter Email:	itmng@kaseya2.com
Organization ID:	us
Machine ID:	
Organization Address:	
Contact:	Benjamin Lavalley
Phone Number:	415-294-5707
Contact Email:	benjamin.lavalley@kaseya.com
Created:	11:33:57 AM 16-Aug-10 (1 minutes ago)
Last Edit:	11:33:57 AM 16-Aug-10 (1 minutes ago)
Promised:	
Closed:	
Escalation:	
Due:	
Status:	Problem
Category:	External Problem
Priority:	Medium
SubCategory:	-- No SubCategory Selected --
Stage:	Logged
Severity:	High
Assigned To:	ben
Policy:	
Owner:	gerald.beaulieu
Root Cause Description:	Consolidation of divions has forced to run on different domains.
Equipment and Service Details:	may need new hardware during consolidation.
Description:	

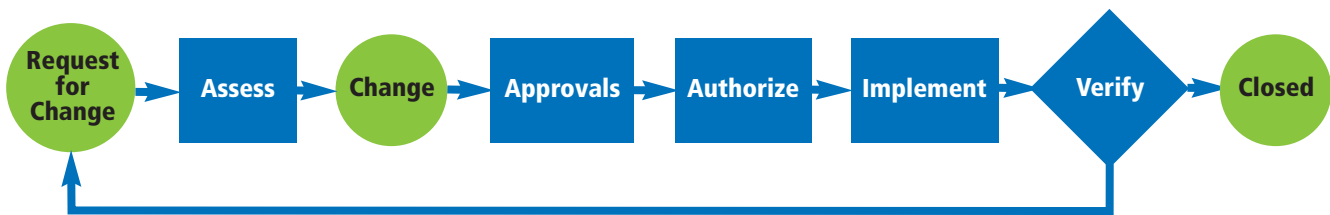


## Change Management

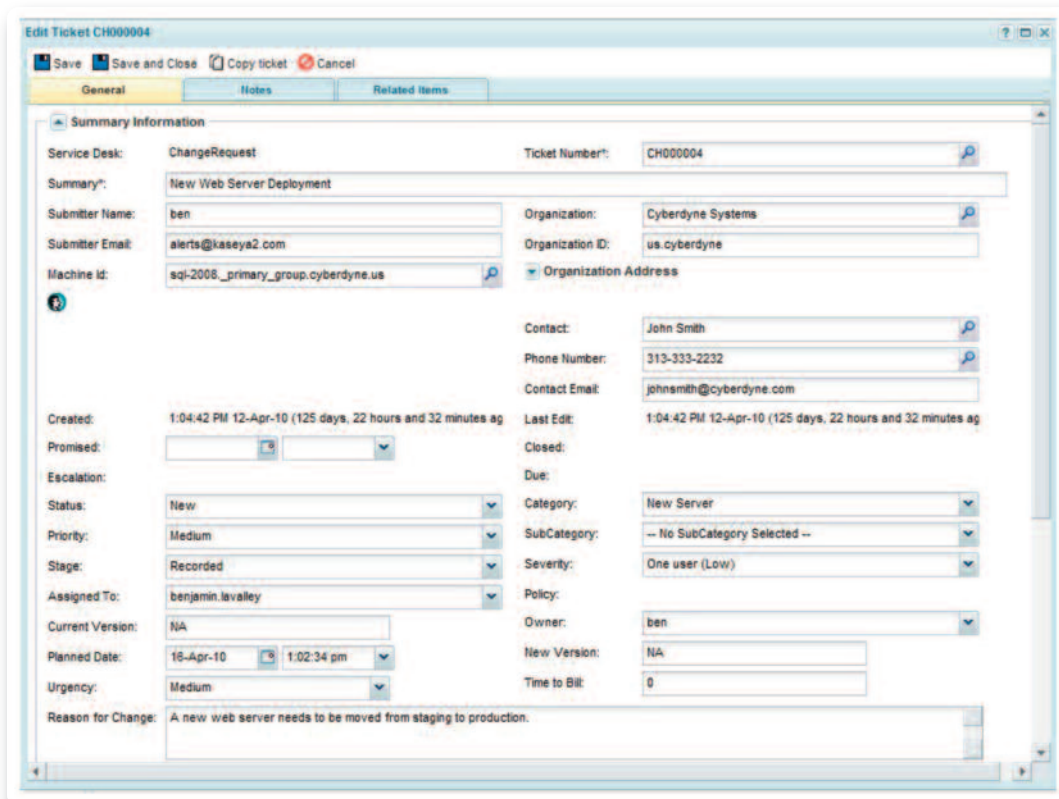
Change is one of the few constants in IT. Hardware breaks. Software drops off support. New releases bring features that IT and our customers cannot resist. The industry changes and we need to respond. Our business changes to take advantage of an opportunity. Change just keeps on happening. And every change brings risk.

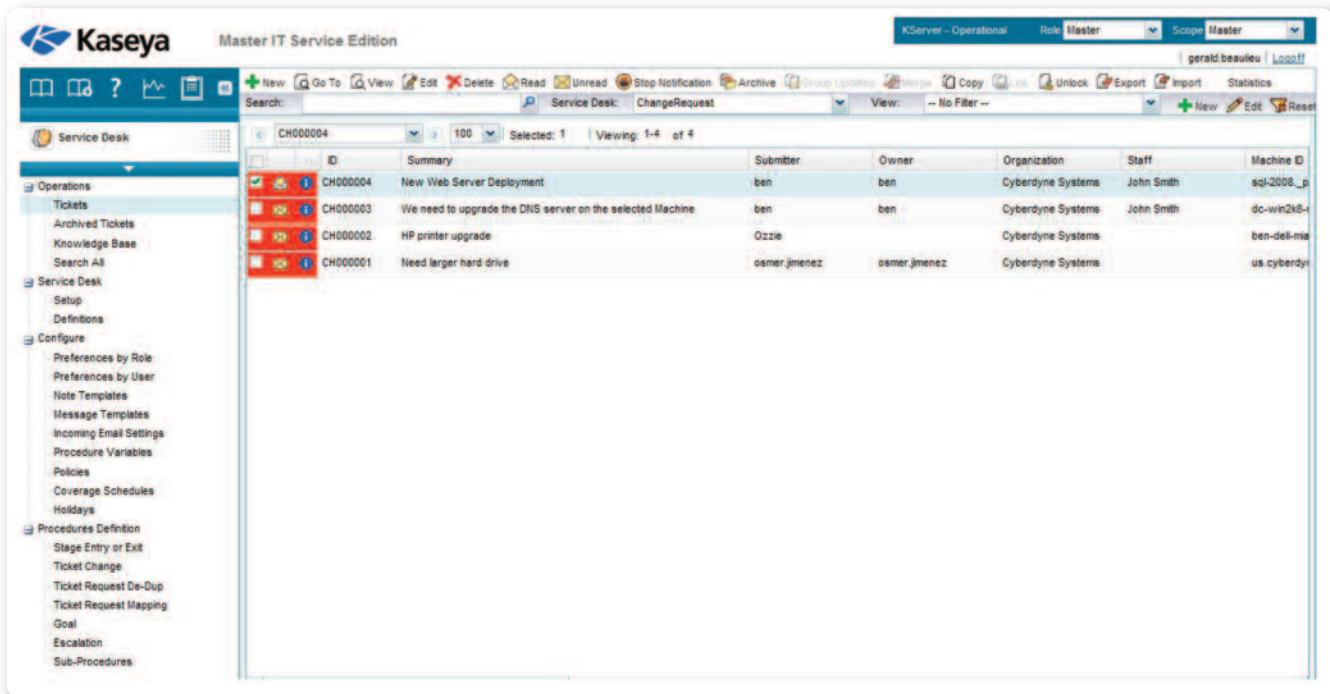
The purpose for Change Management is to manage risk. The Kaseya Service Desk for Change Management addresses that need by giving the Change Manager a consolidated view.

Changes need to be justified. The Kaseya Service Desk suite allows IT to link incidents to problems and problems to changes. This allows the Change Manager to see the justification for changes that are targeted at problem resolution. The Kaseya Service Desk for Change Management also allows the Change Manager to manually enter requests for change for all of the other types of changes that are externally motivated.



The goal for Change Management is to manage risk. The ITIL approach to risk management is to make the changes visible to everyone involved. The Kaseya Service Desk for Change Management is the portal where everyone can view all of the proposed changes. This allows collaborative input regarding the schedule. For example, two updates might be proposed for the same weekend. The Kaseya Service Desk makes it possible for the team reviewing those changes to access the information they need to decide whether to do those changes sequentially or in parallel. If, for example, one proposed change is to apply a service pack to the web servers and another proposed change is to replace the DNS server, the cumulative risk is greater than if either change was made separately. Having a consolidated view of the proposed changes allows management to make the right decisions.





The Kaseya Service Desk for Change Management is also the tool the Change Manager uses to document the approvals that should ultimately lead to the change being authorized. Each person who needs to review the change can use the Kaseya Service Desk for Change Management to see the change implementation plan and the change back-out plan. And the list of change approvers can be customized. For example, submitting a change that will update a database can be configured to automatically send email notification to the database administrator. And submitting a change that will update an application server can be configured to automatically send email notification to the managers responsible for the database it uses, the web servers that use it as well as the manager responsible for application servers. The Kaseya Service Desk for Change Management is highly configurable.

## Summary

The end result is that the IT executives can see the big picture and know what the IT staff is doing. All incidents, requests, problems and changes are consolidated in one place. Status can be quickly ascertained. And with that status, management can ensure the right people are working on the right stuff.

The reports included with this suite make it possible for IT executives to assess and justify headcount so that staffing aligns with the work load. The tools and automation make it possible for the IT team to get more done. And having it all integrated with the Kaseya monitoring tools provides a synergism that amplifies the power of both this suite and the connected tools.

### About the author

With more than 30 years experience, Robert has endeavored to work every role within the realm of IT. He has excelled as a programmer, database administrator, manager, IT Director, college professor, project manager, head of a PMO and book author. He is certified as an ITIL Service Master (ITIL-SM), a Project Management Professional (PMP), a Six Sigma Master Black Belt and a Certified Information Systems Auditor (non-practicing CISA). Robert's goal is to combine the role of visionary, strategist, change-agent and process-proponent while managing initiatives through metrics.

### About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to [www.kaseya.com/download](http://www.kaseya.com/download) for a FREE trial.

Visit: [www.kaseya.com](http://www.kaseya.com) | Email: [sales@kaseya.com](mailto:sales@kaseya.com) | Like: [Facebook.com/KaseyaFan](https://www.facebook.com/KaseyaFan) | Follow: [@KaseyaCorp](https://twitter.com/KaseyaCorp)

